**ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ**
**INFORMATION TECHNOLOGY, COMPUTER SCIENCE, AND MANAGEMENT**




УДК 00.004 https://doi.org/10.23947/1992-5980-2020-20-2-178-187

# Алгоритм работы программного комплекса интеллектуальной поддержки принятия решений при проектировании системы защиты информации на предприятии



**Е. А. Витенбург, А. В. Никишова**
ФГАОУ ВО «Волгоградский государственный университет» (г. Волгоград, Российская Федерация)

*Введение.* Для повышения оперативности принятия решений на предприятии целесообразно использовать специальный программный комплекс интеллектуальной поддержки. Такой продукт необходим при проектировании системы защиты информации и повышении ее неуязвимости в ходе модернизации или изменения конфигурации. Цели исследования: создание алгоритма и математической модели программного комплекса интеллектуальной поддержки принятия решений.
*Материалы и методы.* Метод поддержки принятия решений при проектировании системы защиты информации базируется на использовании нейронной сети (многослойный персептрон). Для объективной оценки исходной защищенности информационной системы (ИС) сформирована математическая модель анализа событий безопасности.
*Результаты исследования*. Проанализирована статистика злоумышленных воздействий на ИС предприятий. Определена необходимость своевременной и точной модернизации системы защиты информации. Важными характеристиками процесса проектирования системы защиты информации являются скорость получения результата и снижение остаточного риска ИС. В связи с этим актуально использование систем искусственного интеллекта в процессе определения лучшего набора подсистем защиты. Классифицированы угрозы нарушения информационной безопасности (ИБ). Определены основные классы событий безопасности. Создана математическая модель нейронной сети, указаны входные параметры ее работы.
Действующая ИС предприятия генерирует многочисленные события, что обусловливает необходимость автоматического сбора и анализа данных с подсистем регистрации объектов ИС. Детально рассмотрен процесс анализа событий безопасности, так как от корректности данных, полученных таким образом, зависит адекватность сгенерированных проектных решений. Сформирован алгоритм работы программного комплекса.
*Обсуждение и заключение*. Полученные результаты могут быть использованы при проектировании системы защиты информации на предприятии. Кроме того, администраторы ИБ могут применить разрабатываемый программный комплекс для корректировки конфигурационных настроек средств защиты информации. Предложенное решение позволит минимизировать деструктивное влияние разработчика системы защиты, который может быть и бывает субъективен.

***Ключевые слова:*** информационная безопасность, информационная система, нейронная сеть проектирования, многослойный персептрон, алгоритм.

***Для цитирования*:** Витенбург, Е. А. Алгоритм работы программного комплекса интеллектуальной поддержки принятия решений при проектировании системы защиты информации на предприятии / Е. А. Витенбург, А. В. Никишова // Вестник Донского государственного технического университета. — 2020. — Т. 20, № 2. — С. 178—187. https://doi.org/10.23947/1992-5980-2020-20-2-178-187

***Финансирование*:** работа выполнена при финансовой поддержке молодых российских ученых Советом по грантам Президента Российской Федерации в рамках НИР «Построение модели интеллектуальной поддержки принятия решений при проектировании системы защиты информации на предприятии».





# Algorithm of software package of intellectual decision support when designing cyber security system at the enterprise

**E. A. Vitenburg, A. V. Nikishova**
Volgograd State University (Volgograd, Russian Federation)

*Introduction.* To increase the decision-making efficiency at the enterprise, it is advisable to use a special software package of intellectual support. Such a product is necessary when designing an information security system and increasing its invulnerability during modernization or configuration changes. Research objectives are as follows: to develop an algorithm and a mathematical model of the software package for intellectual decision support.
*Materials and Methods.* The decision support method under designing an information security system is based on the use of a neural network (multilayer perceptron). For an objective assessment of the initial security of an information system (IS), a mathematical model for the analysis of security events is developed.
*Results.* The statistics of malicious attacks on the IS of enterprises is analyzed. The need for timely and accurate modernization of the information protection system is determined. Important characteristics of the designing an information security system are the speed at which the result is obtained and the reduction in the residual risk of IS. In this regard, the use of artificial intelligence systems in the process of determining the best set of protection subsystems is important. The threats to cyber security (CS) are classified. The main classes of security events are defined. A mathematical model of the neural network is developed; the input parameters of its operation are indicated. The current enterprise IS generates numerous events which necessitates the automatic collection and analysis of data from subsystems for registering IS objects. The process of analyzing security events is considered in detail since the adequacy of the generated design decisions depends on the correctness of the data obtained in this way. The algorithm of the software package is formed.
*Discussion and Conclusions.* The results can be used in the design of the information security system at the enterprise. In addition, CS administrators can use the developed software package to adjust the configuration settings of information security tools. The proposed solution will minimize the destructive influence of the developer of the security system which may and happen to be subjective.

***Keywords****:* cyber security, information system, neural network engineering, multilayer perceptron, algorithm.

***For citation:*** E. A. Vitenburg, A. V. Nikishova. Algorithm of software package of intellectual decision support when designing cyber security system at the enterprise. Vestnik of DSTU, 2020, vol. 20, no. 2, pp. 178—187. https://doi.org/10.23947/1992-5980-2020-20-2-178-187

***Funding information*****:** the research is done with the financial support of young Russian scientists from the Grants Council of President of the Russian Federation in R&D on “Building a model of intellectual decision-making support when designing an information security system at the enterprise”.

**Введение.** С развитием промышленности в России растет число предприятий, отнесенных к объектам критической информационной инфраструктуры (ОКИИ). Статистика распространения атак от вендора Positive Technologies[1] показывает рост количества успешно реализованных злоумышленных воздействий в этой сфере. В 2019 году зафиксировано 125 атак на промышленные информационные системы (ИС). Это более чем в три раза (или на 212%) превосходит аналогичный показатель 2018 года (40 атак). Диаграмма распределения количества атак по кварталам года (Q) приведена на рис. 1.

[1]Актуальные киберугрозы: IV квартал 2019 года / Positive Technologies. URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2019-q4 (дата обращения: 24.02.2020).

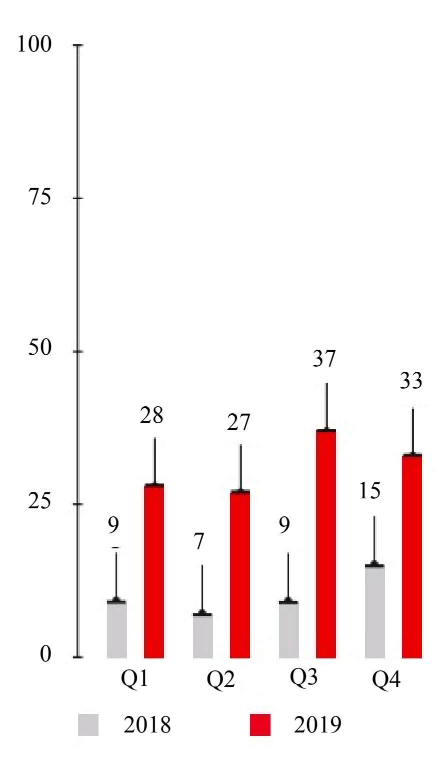



Рис. 1. Число атак на ИС предприятий в 2018 и 2019 году

Промышленные ИС атакуют преимущественно с использованием вредоносного программного обеспечения (90 % атак). Данную сферу курируют Федеральная служба безопасности и Федеральная служба по техническому и экспертному контролю. Необходимость обеспечения информационной безопасности (ИБ) промышленных информационных систем подтверждается статистикой ведущих аналитических центров [1]. Согласно нормативно-правовым актам Российской Федерации[2], владельцы ОКИИ задействуют комплекс организационно-технических мероприятий для обеспечения безопасного функционирования информационной инфраструктуры. При этом законодательством предусмотрена периодическая ревизия качества функционирования системы защиты информации (СЗИ), оценка ее эффективности. Этим обусловлена необходимость оперативной корректировки конфигурационных настроек имеющихся средств или доукомплектация системы инструментами защиты информации. Особую роль играют оперативность и точность принимаемых решений, а величина остаточного риска не должна превышать установленные показатели [2]. В связи с этим предлагается автоматизировать процедуру поддержки принятия решений при проектировании СЗИ на предприятии.

**Материалы и методы.** Для поддержки принятия решений при проектировании СЗИ применен метод, основанный на нейронной сети (многослойный персептрон) [3]. Входные данные для работы нейронный сети — угрозы нарушения информационной безопасности и события безопасности. Кроме того, для объективной оценки исходной защищенности информационной системы сформирована математическая модель анализа событий безопасности. В рамках этой модели рассчитанные меры сходства ИС сравниваются с одним из уровней безопасности ИС. В качестве метрики сходства используется взвешенное расстояние Манхэттена.

**Результаты исследования.** В рамках данного исследования предложен подход к проектированию системы защиты, основанный на показателях важности подсистем защиты информации, входящих в СЗИ [4]. С учетом этих данных предлагается формировать перечень средств защиты наиболее важных подсистем. Данный подход позволяет усилить СЗИ за счет нейтрализации актуальных угроз. При этом актуальность следует определять, исходя из автоматизированного анализа событий безопасности [5, 6]. Вектор важности подсистем защиты информации формируется в соответствии с выражением

$$V = S(Class_Thr), \quad (1)$$

где $V = (V_1, \dots, V_9)$ — вектор важности подсистем СЗИ; $Class_Thr = (Class_Thr_1, \dots, Class_Thr_6)$ — вектор актуальности классов угроз; $S$ — функциональная зависимость, определенная нейронной сетью.

[2] О безопасности критической информационной инфраструктуры Российской Федерации : федер. закон от 26 июля 2017 г. № 187-ФЗ / Государственная Дума РФ, Совет Федерации // ФСТЭК России. URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/obespechenie-bezopasnosti-kriticheskoj-informatsionnoj-infrastruktury/285-zakony/1610-federalnyj-zakon-ot-26-iyulya-2017-g-n-187-fz (дата обращения: 18.05.20).

Множество угроз $Thr$ нарушения ИБ для удобства разделим на классы $Class_Thr$, которые определяются, как в [6]:

$$Class_Thr = \{ Thr_Br, Thr_L, Th_Dist, Thr_Loss, Thr_B, Thr_A\}, \quad (2)$$

где $Thr_Br$ — класс угроз нарушения ИБ типа «взлом»; $Thr_L$ — класс угроз нарушения ИБ типа «утечка»; $Th_Dist$ — класс угроз нарушения ИБ типа «искажение»; $Thr_Loss$ — класс угроз нарушения ИБ типа «утрата»; $Thr_B$ — класс угроз нарушения ИБ типа «блокирование»; $Thr_A$ — класс угроз нарушения ИБ типа «злоупотребление».

Для формирования вектора актуальности угроз нарушения ИБ ИС предлагается формировать две матрицы соответствия:

— множества угроз множеству классов угроз — $MThr$,

— множества событий безопасности классам угроз — $MEvent$.

Матрица $MThr$:

$$MThr = Thr \times Class_Thr = (mth_{ij}). \quad (3)$$

Здесь $mth_{ij}$ определяется по формуле:

$$mth_{ij} = \begin{cases} \frac{1}{n}, \text{если угроза принадлежит классу угроз,} \\ 0 \text{ в противном случае.} \end{cases} \quad (4)$$

Здесь $n$ — количество классов угроз, которым принадлежит угроза.

При этом $\forall i, \sum_j mth_{ij} = 1$.

Матрица $MEvent$:

$$MEvent = Events \times CThr = (mev_{ij}). \quad (5)$$

Здесь $mev_{ij}$ определяется по формуле:

$$mev_{ij} = \begin{cases} 1, \text{если событие возникает при реализации угрозы класса,} \\ 0 \text{ в противном случае.} \end{cases} \quad (6)$$

Для формирования вектора важности подсистем защиты информации предлагается использовать в программном комплексе нейронную сеть — многослойный персептрон, функционирующий согласно формуле, приведенной в [7]:

$$\begin{cases} In_{0k} = v_k \\ Out_{ij} = f(\sum_l w_{ijl} In_{ijl} - \theta_{ij}), \\ In_{ijl} = Out_{i-1l} \end{cases} \quad (7)$$

где $In_{0k}$ — $k$-й нейрон входного слоя; $v_k$ — $k$-й элемент входного вектора; $Out_{ij}$ — выходное значение $j$-го нейрона $i$-го слоя; $f$ — функция активации нейрона, которая определяется функциональной зависимостью $V(1)$; $w_{ijl}$ — вес $l$-го входа $j$-го нейрона $i$-го слоя; $In_{ijl}$ — значение $l$-го входа $j$-го нейрона $i$-го слоя; $\theta_{ij}$ — уровень активации $j$-го нейрона $i$-го слоя; $Out_{i-1l}$ — выходное значение $l$-го нейрона ($i$ – 1)-го слоя.

На этапе анализа событий безопасности исходными данными являются журналы событий безопасности, которые создает системное и прикладное программное обеспечение ИС предприятия. Множество событий безопасности *Events* включает в себя следующие классы [8]:

$$Events = \{EnterEv, ManagementSubEv, AccessObjEv, PolicyChangeEv, \\ UsePrivilegesEv, ISProcessesEv, LevelISEv\}. \quad (8)$$

Здесь $EnterEv$ — события класса «вход субъектов в систему»; $ManagementSubEv$ — события класса «управление субъектами»; $AccessObjEv$ — события класса «получение доступа к объектам»; $PolicyChangeEv$ — события класса «изменения политики системы»; $UsePrivilegesEv$ — события класса «использование субъектом особых привилегий»; $ISProcessesEv$ — события класса «функционирование процессов системы»; $LevelISEv$ — события класса «уровень системы».

Из множества событий выбираются опасные. Для сопоставления множества опасных событий с классами угроз используются матрицы соответствия. Матрица, сформированная в рамках данного исследования, представлена в табл. 1.

Таблица 1

Матрица соответствия угроз нарушения ИБ ИС предприятия

| Класс события безопасности | Типы угроз | | | | | | |
|---|---|---|---|---|---|---|---|
| | $EnterEv$ | $ManagementSubEv$ | $AccessObjEv$ | $PolicyChangeEv$ | $UsePrivilegesEv$ | $ISProcessesEv$ | $LevelISEv$ |
| $Thr_Br$ | + | | + | | + | | |
| $Thr_L$ | | | + | | | + | |
| $Th_Dist$ | + | | | | | + | |
| $Thr_Loss$ | | | + | | | + | |
| $Thr_B$ | | + | | | | | + |
| $Thr_A$ | + | + | | + | + | | + |

Затем формируется вектор актуальных классов угроз нарушения ИБ ИС. После этого актуальным классам угроз противопоставляются подсистемы СЗИ. Соответствие определяется с помощью нейронной сети с учетом функциональной зависимости $V$ в соответствии с формулой (1).

Немаловажным фактором является количество анализируемых наборов событий и их источников. При этом стоит отметить, что количество событий безопасности прямо пропорционально количеству источников — информационных ресурсов ИС предприятия [8]. С учетом большого числа событий, генерируемых работающей ИС, актуально проводить автоматический сбор и анализ данных с подсистем регистрации объектов ИС, описывающих события. В связи с этим стоит подробно рассмотреть анализ событий безопасности, так как от корректности полученных на этом этапе выводов зависит адекватность сгенерированных проектных решений.

Согласно [9, 10], в определенный момент времени $T$ текущее состояние ИС предприятия $S_T \in State, State = \{Snorm, Sdang, Sanorm\}$ можно охарактеризовать как:

— нормальное ($Snorm$) — штатное функционирование системы в соответствии с ее задачами и согласно документам, регламентирующим работу;

— опасное ($Sdang$) — некорректное функционирование ИС, фиксируются нарушения работы, связанные с атаками злоумышленника, сбоями и отказами программного и (или) технического обеспечения;

— аномальное ($Sanorm$) — временное изменение штатного режима функционирования ИС и всплеск аномальной активности пользователей, программ и сетевого трафика.

Более детального анализа требуют опасные и аномальные события. Набор такого рода событий — это входные данные этапа сопоставления классов угроз. Такие события свидетельствуют о реализации угроз безопасности.

Следовательно, входными данными для нейронной сети (7) будут результаты мониторинга и анализа событий безопасности.

Любое событие безопасности $EventIS_i$ может быть описано кортежем атрибутов [9]:

$$EventIS_i = \langle ID, Data, Level, Source, EventType, EventState, SecureParams \rangle, \quad (9)$$

где $ID$ — код события; $Data$ — время генерации события; $Level$ — уровень опасности события; $Source$ — источник возникновения события; $EventType$ — тип события; $EventState$ — состояние события; $SecureParams$ — вектор параметров безопасности события.

$$SecureParams = \langle h, u, risk \rangle, \quad (10)$$

где $h$ — показатель возникновения события определенного кода относительно общего количества событий безопасности за период $\Delta T$; $u$ — тяжесть последствий события (потенциальный ущерб); $risk$ — риск нарушения информационной безопасности ИС.

За период $\Delta T$ в информационной системе генерируется множество событий ИС (*EventIS*), которые необходимо оценивать для определения уровня защищенности ИС. Соотношение числа событий того или иного типа к общему количеству определяет показатель $h$:

$$h = \frac{NEventID}{NEvent}, \quad (11)$$

где *NEvenID* — количество событий определенного кода, *NEvent* — общее число событий за период $\Delta T$.

Прикладные программные продукты по-разному определяю коды событий. Так, в рамках данной работы рассмотрена кодировка ОС Windows корпорации Microsoft[3].

Риск нарушения информационной безопасности ИС — это функция от частоты реализации события и потенциального ущерба:

$$risk = h \times u. \quad (12)$$

Сумма частных показателей позволяет определить общий риск $RiskSum$:

$$RiskSum = \sum_{i=1}^{EventID} risk_i. \quad (13)$$

Множество, обеспечивающее классификацию событий и оценку частных показателей безопасности ИС, описывается подмножествами элементов:

$$PPS = \{\{EvType\}, \{EvState\}, \{ISState\}\}. \quad (14)$$

Здесь *EvType* — множество типов обнаруженных событий, *EvState* — множество возможных состояний событий:

$$EvState = \{Ev^n, Ev^d, Ev^a\}, \quad (15)$$

где $Ev^n$ — события нормального функционирования ИС; $Ev^d$ — события нарушения ИБ ИС; $Ev^a$— аномальные события, характеризующие отклонения ИС от штатного режима функционирования (нуждаются в дополнительном анализе).

Для определения принадлежности события $EventIS_i$ к одному из трех состояний *EvState* решается задача классификации — используется множество $SP = DamgeEv \cup NormEv$, разделяющееся на два базовых подмножества. Они формируются экспертной группой на основании данных о типовых событиях штатного режима функционирования ИС и ранее обнаруженных атаках и инцидентах ИБ, описывающих сигнатуру типовых для данной ИС и опасных событий:

— $DamgeEv$ — множество событий, которые являются известными признаками атаки или определяют сценарий развития инцидента;

— $NormEv$ — множество событий, характерных для штатного режима функционирования ИС.

$F(EventIS_i(EvState) \to \{SP\}_j)$ классифицируются следующим образом:

$$EventIS_i(EvState) = \begin{cases} Ev^n, EventIS_i \in NormEv, \\ Ev^d, EventIS_i \in DamageEv, \\ Ev^a, EventIS_i \notin NormEv \cup DamageEv. \end{cases} \quad (16)$$

Здесь $EventIS_i(EvState)$ — события ИС с атрибутом состояния, каждому из которых соответствует набор связей $SP_j$ с типовыми событиями из множества шаблонов штатного режима и режима с нарушением ИБ.

Если событие отсутствует в профилях штатных событий или событий нарушения безопасности, оно определяется как аномальное. Причины его возникновения должны отдельно рассматриваться администратором системы ИБ.

*ISState* ={*ISnorm, ISdang,ISanorm*} — множество состояний ИС, указывающее на штатный режим функционирования ИС. Состояние ИС определяется по формуле:

[3]Описание событий системы безопасности в Windows 7 и Windows Server 2008 R2 / Microsoft. URL: https://support.microsoft.com/ru-ru/help/977519/description-of-security-events-in-windows-7-and-in-windows-server-2008 (дата обращения: 05.08.2019).

$$ISState = \begin{cases} ISnorm, \forall EventIS_i \in EventIS | EvState = Ev^n, \\ ISdang, \exists EventIS_i \in EventIS | EvState_i = Ev^d, \\ ISanorm, ISnorm \cap ISdang, \end{cases} \quad (17)$$

где *ISnorm* — режим нормального функционирования ИС; *ISanorm* — режим функционирования ИС с признаками аномальной активности; *ISdang* — режим с зафиксированными нарушениями безопасности ИС (рис. 2).

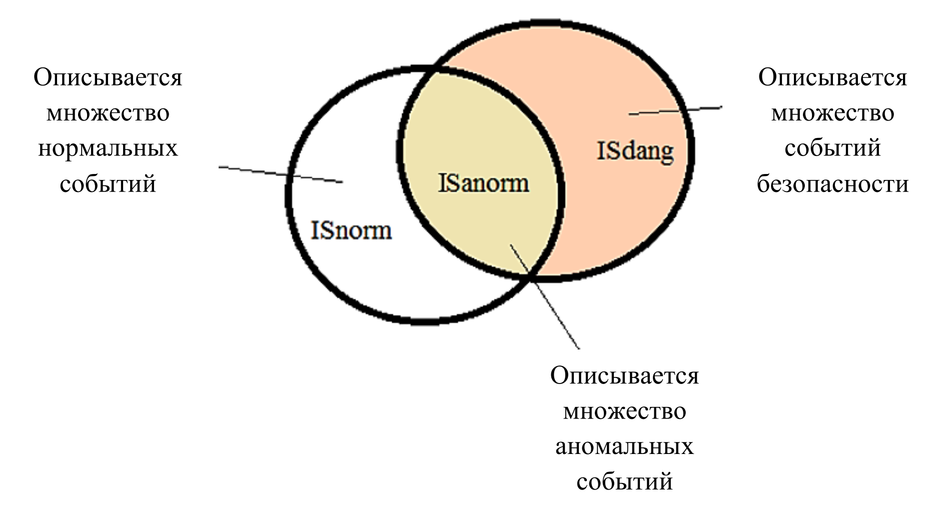



Рис. 2. Отношения подмножеств состояний ИС

С учетом полученных данных формируется вектор, определяющий состояние ИС, суммарный риск, а также долю аномальных событий и событий нарушения безопасности:

$$IS = \langle ISState, RISKsum, NanalEv, NdandEv \rangle, \quad (18)$$

где $NanalEv$ — доля обнаруженных аномальных событий, $NdandEv$ — доля событий нарушения ИБ ИС предприятия.

Для принятия решения о необходимости усиления подсистем защиты информации рассчитывается уровень безопасности ИС *SL:*

$$SL = \{\text{безопасное}, \text{стабильное}, \text{аномальное}, \text{кризисное}, \text{опасное}\}.$$

Для определения уровня безопасности ИС проектировщик системы ИБ формирует вектор, определяющий эталонный показатель защищенности ИС $IS_Perf$. $SL$ формируется на основании сходства векторов $IS$ и $IS_Perf$.

Для оценки безопасности ИС в рамках данной математической модели принято пять уровней, поэтому при определении принадлежности ИС к одному из уровней применен метод $k$ ближайших соседей [10]. С этой целью составляются вспомогательные векторы, соответствующие оставшимся четырем уровням безопасности. Выполнение данной операции базируется на значениях вектора $IS_Perf$, соответствующего безопасному уровню состояния ИС при умножении на скалярный корректирующий коэффициент (значение определяется экспертным путем):

$$k \times RIS = \langle k \times ISState, k \times RISKsum, k \times NanalEvent, k \times\times\ NdandEvent \rangle. \quad (19)$$

В качестве метрики сходства используется взвешенное расстояние Манхэттена [10]:

$$\rho(IS, RIS) = w \sum_{j=1}^{4} |IS_j - RIS_j|. \quad (20)$$

На основании представленной математической модели разработан обобщенный алгоритм работы программного прототипа (рис. 3).

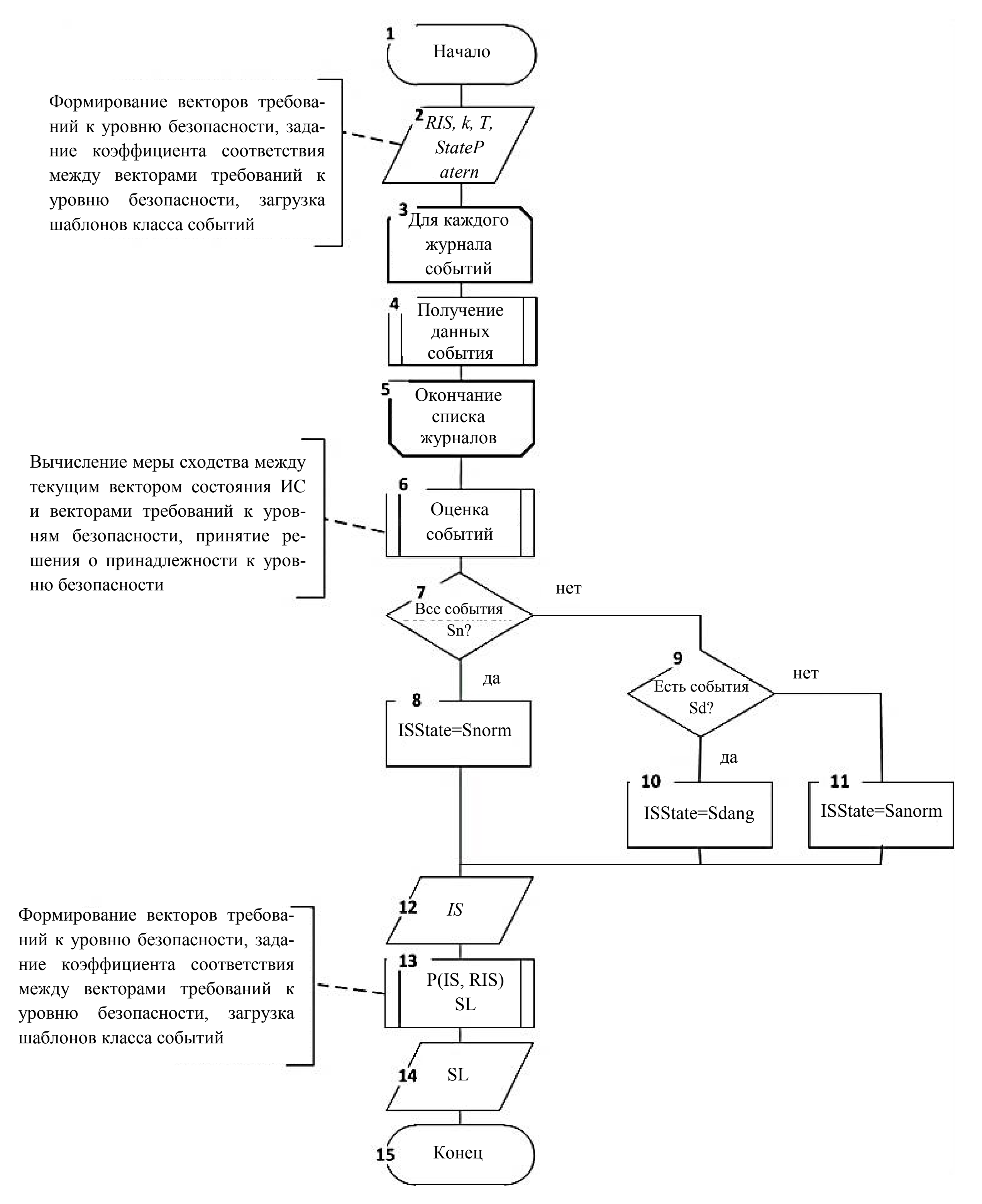



Рис. 3. Алгоритм работы программного прототипа комплекса интеллектуальной поддержки принятия решений при проектировании системы защиты информации на предприятии

Шаг 1 (блоки 1, 2). Запуск программного прототипа. Начало алгоритма. Ввод входных данных о векторах требований $IS_Perf$ к состоянию ИС каждого уровня безопасности. Ввод периода, через который будет проводиться мониторинг. Загрузка из БД шаблонов с множествами нормальных и опасных событий.

Шаг 2 (блоки 3–5). Мониторинг журналов событий ОС, получение записей о каждом событии. Формирование списка событий.

Шаг 3 (блок 6). Анализ данных о собранных событиях, формирование кортежа событий — формула (8). Классификация событий по формулам (14–15) на нормальные, аномальные и опасные. Расчет частоты возникновения событий, потенциального ущерба и риска по формулам (11–13).

Шаг 4 (блоки 7–11). Классификация состояний ИС по формуле (17) на основе данных о распределении событий на множество аномальных, нормальных и опасных (шаг 3).

Шаг 5 (блоки 12–14). На основании рассчитанных данных и кортежей событий в ИС формирование вектора текущего состояния, вычисление мер сходства между векторами $IS$ и $IS_Perf$: формулы (19), (20). Принятие решения о принадлежности ИС к одному из пяти уровней безопасности.

Шаг 6 (блок 15). Завершение алгоритма.

**Заключение.** В рамках данного исследования предложен подход к моделированию системы защиты информации. Учитывается различный качественный и количественный состав средств защиты в зависимости от актуальных угроз нарушения информационной безопасности. Представленный метод позволяет повысить эффективность работы внедряемой системы защиты информации и уменьшить вероятность ошибки проектировщика. Программный комплекс, создаваемый в рамках данного исследования, обладает преимуществами, которые невозможно получить при «ручном» проектировании:

— учет всех данных о защищаемой системе,

— получение точных результатов в максимально короткий срок.

**Библиографический список**

1. Майорова, Е. В. Методические аспекты реагирования на инциденты информационной безопасности в условиях цифровой экономики / Е. В. Майорова // Петербургский экономический журнал : [сайт]. — 2020. — № 1. — URL: https://cyberleninka.ru/article/n/metodicheskie-aspekty-reagirovaniya-na-intsidenty-informatsionnoy-bezopasnosti-v-usloviyah-tsifrovoy-ekonomiki (дата обращения: 24.02.2020).

2. Применение методов теории нечетких множеств к оценке рисков нарушения критически важных свойств защищаемых ресурсов автоматизированных систем управления / А. И. Братченко, И. В. Бутусов, А. М. Кобелян, А. А. Романов // Вопросы кибербезопасности : [сайт]. — 2019. — № 1 (29). — URL: https://cyberleninka.ru/article/n/primenenie-metodov-teorii-nechetkih-mnozhestv-k-otsenke-riskov-narusheniya-kriticheski-vazhnyh-svoystv-zaschischaemyh-resursov (дата обращения: 24.04.2020).

3. Витенбург, Е. А. Математическая модель интеллектуальной поддержки принятия решений при проектировании системы защиты информации на предприятии / Е. А. Витенбург // Промышленные АСУ и контроллеры. — Москва : Научтехлитиздат, 2019. — С. 54–60.

4. Витенбург, Е. А. Выбор элементов комплекса защиты информационной системы предприятия на основе требований нормативно-правовых документов / Е. А. Витенбург, А. А. Левцова // Вестник Донского государственного технического университета. — 2018. — № 3. — С. 333–338.

5. Степанова, Е. С. Разработка модели угроз на основе построения нечеткой когнитивной карты для численной оценки риска нарушения информационной безопасности / Е. С. Степанова, И. В. Машкина, В. И. Васильев // Известия ЮФУ. Технические науки : [сайт]. — 2010. — № 11. — С. 31–40. — URL: https://cyberleninka.ru/article/n/razrabotka-modeli-ugroz-na-osnove-postroeniya-nechetkoy-kognitivnoy-karty-dlya-chislennoy-otsenki-riska-narusheniya-informatsionnoy (дата обращения: 24.04.2020).

6. Витенбург, Е. А. Модель угроз информационной системы предприятия / Е. А. Витенбург, А. А. Левцова // Промышленные АСУ и контроллеры. — 2018. — № 9. — С. 46–50.

7. Бова, В. В. Применение искусственных нейронных сетей для коллективного решения интеллектуальных задач / В. В. Бова, А. Н. Дуккарт // Известия ЮФУ. Технические науки. — 2012. — № 7 (132). — С. 131–138.

8. Смоляк, Д. С. Мониторинг событий информационной безопасности техногенных объектов / Д. С. Смоляк, Т. А. Пулко // Доклады Белорусского государственного университета информатики и радиоэлектроники. — Минск : Изд-во Белорус. гос. ун-та информатики и радиоэлектроники, 2015. — С. 43–47.

9. Использование методов системного анализа для решения проблемы обеспечения безопасности современных информационных систем / И. В. Машкина, А. Ю. Сенцова, М. Н. Гузаиров, В. Е. Кладов // Известия ЮФУ. Технические науки. 2011. — № 12 (125). — С. 25–35.

10. Астрахов, А. В. Противодействие компьютерным атакам. Технологические основы. Электронное учебное издание : [сайт] / А. В. Астрахов, С. М. Климов, М. П. Сычев. — Москва : МГТУ имени Н. Э. Баумана, 2013. — 70 с. — URL: http://wwwcdl.bmstu.ru/iu10/comp-atak-techno.pdf (дата обращения: 18.05.2020).

Сдана в редакцию 27.03.2020
Запланирована в номер 27.04.2020

*Об авторах:*

**Витенбург Екатерина Александровна,** аспирант кафедры «Информационная безопасность», ФГАОУ ВО «Волгоградский государственный университет» (400062, РФ, г. Волгоград, пр. Университетский, 100), ResearcherID: N- O-8740-2017, ScopusID 57209346586, ORCID: https://orcid.org/0000-0002-1534-8865, e.vitenburg@ec-rs.ru

**Никишова Арина Валерьевна,** доцент кафедры «Информационная безопасность», ФГАОУ ВО «Волгоградский государственный университет» (400062, РФ, г. Волгоград, пр. Университетский, 100), кандидат технических наук, ResearcherID: N-3217-2016, ScopusID 57201358403, ORCID: https://orcid.org/0000-0002-0919-2593, nikishova.arina@volsu.ru

*Заявленный вклад соавторов*

Е. А. Витенбург — формирование основной концепции, определение целей и задач исследования, создание математического аппарата обработки событий безопасности, формулирование выводов. А. В. Никишова — научное руководство, анализ результатов исследования, разработка математического аппарата интеллектуальной поддержки принятия решений, корректировка выводов.

*Все авторы прочитали и одобрили окончательный вариант рукописи.*